Bermuda's new privacy legislation: are you prepared?

By Kathleen Moniz, Conyers Dill & Pearman

For any organisation, personal information about customers, clients, employees and suppliers is a valuable asset. But it is also a responsibility. Protecting the privacy of personal information is not just a hot topic on the internet, it is now every Bermuda organisation's legal duty.

The Personal Information Privacy Act 2016 (PIPA), which will come into force in the latter part of 2018, affects every individual and organisation that uses personal information in Bermuda, including companies, charities and Government. It imposes a number of requirements for the safeguarding and use of personal information - and significant penalties for non-compliance – so businesses need to be prepared.

Why was PIPA introduced?
Across the world, there is a move towards increasingly stringent regulation putting the onus on organisations to protect individual privacy by safeguarding any personal information that they hold. PIPA is intended to ensure that Bermuda is part of the international 'network of trust' between countries with similar levels of privacy protection. For example, the European Union's General Data Protection Regulation (GDPR) came into force this month. PIPA should ensure that Bermuda meets the GDPR's standard of 'adequacy' that will allow the free flow of personal data from the EU to Bermuda without additional conditions being imposed.

What counts as Personal Information?

'Personal information' is any information about an identified or identifiable individual. PIPA encompasses information in both digital and non-digital (paper) forms and defines its 'use' very broadly to include collection, storage, disclosure, transfer and destruction.

'Sensitive personal information' which includes information about an individual's race, health, family status or religious beliefs, is a separate class of personal information and is subject to enhanced protection. Employee data inevitably includes much of this information. Businesses should pay particular attention to the appropriate collection, handling and secure storage of this data.

What are the key requirements?

Safeguarding privacy means managing risks. Every organisation is required to have suitable policies and practices with regards to the protection and use of personal information and should make sure their employees are aware of them. They must:

- Ensure personal information is held securely with 'appropriate safeguards' against risks such as loss and unauthorised access, and misuse such as unauthorised disclosure or destruction.
- Use personal information in a 'lawful and fair manner', for specific purposes only and in accordance with the rights of individuals. Information held should not be excessive for the purpose, should be accurate and up-to-date and not held for longer than necessary.
- Notify the Government-appointed Privacy Commissioner promptly in the event of a security breach leading to the loss, destruction or unauthorised disclosure of personal information which is likely to adversely affect individuals.
- Assess the protection provided by any third parties engaged to use or handle the information. The primary organisation remains responsible for compliance. Personal information should not be transferred outside Bermuda without adequate checks and safeguards.

What are the penalties for non-compliance?

PIPA establishes a number of offences and penalties for failure to comply with the Act, including fines of up to $250,000 for organisations, and up to $25,000 or imprisonment up to two years for individuals.

How to prepare

It is a good idea to seek legal advice to ensure you are ready to meet your data protection obligations. Assistance can range from advice on legal duties and risks to privacy policy implementation.

Kathleen Moniz is an Associate in the Corporate Practice of Conyers Dill & Pearman ■